APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/576,975	04/20/2006	Holger Krummel	851.0015.U1(US)	8160

29683   7590   05/04/2009
HARRINGTON & SMITH, PC
4 RESEARCH DRIVE, Suite 202
SHELTON, CT 06484-6212

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
05/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/576,975	KRUMMEL ET AL.
Office Action Summary	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>30 March 2009</u>.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-30 and 34-37* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) *1-30, 34-37* is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All b) ☐ Some * c) ☐ None of:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/30/09 has been entered.

Claims 1, 3, 5, 7, 11-12, 14-16, 18, 21-22, 24, 29, and 34-35 have been amended. Claims 36 and 37 have been added. Therefore, claims 1-30 and 34-37 remain pending.

Response to Amendment

Claim Rejections - 35 USC § 101

The current amendments overcome the previous 101 rejection.

Claim Rejections - 35 USC § 112

The current amendments overcome the previous 112 rejection.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 7 is rejected as being indefinite because it contradicts a limitation of claim 1. As claim 1 reads, the secret is made available at the first apparatus without contemporaneous user input. Claim 7, explicitly referring to and narrowing this limitation, then recites prompting a user for input at the first apparatus. Claim 1 can be interpreted as not requiring user input at the first and/or second apparatus. If one interprets the absence of user input at the first apparatus then claim 7 contradicts claim 1. If one interprets the absence of user input at the second apparatus then claim 7 would not contradict claim 1. Also a user input is newly defined but user input is already defined in claim 1. Are they the same user input?

Response to Arguments

Applicant's arguments filed 3/30/09 have been fully considered but they are not persuasive. It appears from the Applicant's response that the Applicant has misinterpreted the Examiner's interpretation of the cited prior art, Ma. Examiner will clarify the interpretation of the prior art and expound upon how those limitations teach the claim's limitations.

As per claim 1, the second apparatus and first apparatus are equivalent to the first and second wireless communication device of paragraph 0032. In this paragraph the second device controls access to both the wireless network between said devices and between the first device and the wireless network. The first device cannot establish and secure connection without first authenticating with the second device. Therefore the second device controls access to the communication networks. Next, the second device holds the SIM card in it. The SIM is where there keys are stored. Ma teaches the keys are used for establishing the authenticated channel between said devices (0032). As per the stored secret, this can be attributed to the secret needed to be shared between the devices in order to begin the pairing process. As Ma teaches, pairing can be performed by entry of a password into the first device. It requires no contemporaneous user input at the second device in order to make the secret available at the first device. The claim loosely couples the use of the secret with creating the secret key. As broadly interpreted, this limitation does not require the secret to be an input into the creation of the secret key. The secret is used by virtue of the pairing process between the first and second devices. Ma teaches the pairing process identifies one or more keys to be used in the authenticated channel between the first and second devices (0032). Lastly, the stored secret being associated with an operational mode is another loosely coupled relationship. Examiner interprets this limitation to mean the secret is needed to perform an operational mode of the second device. Ma teaches the secret is used to pair the two devices. Pairing the two is essential to permit the first device to access the carrier network. Therefore the secret

key is associated with the first device becoming operational (0032; last sentence and

0037). The first device is therefore able to operate in a mode in which the second

device was able to operate in. Examples taught by Ma include voice and data

communications.

Now summarizing, Examiner interprets the pairing functions of the first and

second device (Ma; paragraph 0032) to read on the limitations of the independent

claims. Examiner finds the second device to control access to a radio communication

network.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 4-15, 17-24, 26-30, 34, 35, and 37 are rejected under 35 U.S.C.

102(e) as being anticipated by USP Application Publication 2005/0021940 to Ma,

hereinafter Ma.

As per claim 1, Ma teaches a method, comprising:

storing in a second apparatus [second device] which controls access to a radio communications network a secret generated at the second apparatus, wherein the stored secret [password] is associated with an operational mode of the second apparatus (0032);

making the stored secret available at a first apparatus without contemporaneous user input [told to (or known) by the user of the first apparatus which then inputs it into the first apparatus but does not need to be inputted into the second device; 0032; also taught in 0037 where it can be remembered and automatically input]; and

creating in the second apparatus, using the secret, a secret key for use in pairing the first and second apparatus to secure communication between them (0032).

As per claim 2, Ma teaches the secret is previously generated at the second apparatus by user input to the second apparatus [PINs are chosen and stored in SIM card on smartphone] (0027 and 0033).

As per claim 4, Ma teaches wherein the stored secret is associated with a service provided by the device [allow for operation of service if PIN matches] (0033).

As per claim 5, Ma teaches determining that the signal is associated with the operational mode of the second apparatus [wants to use the data in the SIM to access the carrier network] receiving a signal from the first device and in response to the received signal, automatically creating without user intervention the secret key [automatic pairing of devices when correct PIN is received] (0039).

As per claim 6, Ma teaches making the stored secret available at the first device

is without communication in the network [PIN is not transmitted from second device to

first device, user of first device must know PIN in order to authenticate] (0039).

As per claim 7, Ma teaches making the stored secret available at the first device

involves prompting a user input of the secret to the first device [user inputs PIN via input

device] (0039).

As per claim 8, Ma teaches storing in the second device an identifier of the first

device and an identifier of the second device [identifying information of the first device is

stored in SIM of the second device for automatic pairing] (0039).

As per claim 9, Ma teaches the step of creating the secret key uses a random

number communicated between the first and second devices [use of random number

helps secure the authentication process] (0029).

As per claim 10, Ma teaches the step of creating the secret key uses an identifier

of one of the first and second devices, communicated between the first and second

devices, in the creation of the secret key [secure pairing using identifying information of

the devices so that automatic pair can later occur simply when the two devices are in

range of one another] (0037). Ma specifically mentions that the signal includes the

identifying information.

As per claim 11, Ma teaches re-using the stored secret to join a third device to

the radio communications network without contemporaneous user input of a secret at

the second device, comprising: making the stored secret [PIN] available at the third

device; and creating in the second device, using the secret, a secret key (0032); and

Making the secret key available to the third apparatus for use in pairing the third

and second apparatus to secure communication between them [a plurality of devices

can perform the same pairing to the second device as the first device] (0034).

As per claim 12, Ma teaches a method of joining a plurality of first devices to a

radio communications network controlled by a second device, comprising:

storing in the second device a generated secret [PIN] at the second device which

controls access to a radio communications network (0032) wherein the stored secret is

associated with an operational mode of the second apparatus (0032; last sentence and

0037);

making the stored secret available to each of the first devices [input by users of

the plurality of first devices; 0032]; and

creating in the first devices and in the second device, using the secret, at least

one secret key [secure pairing via keys] for use in securing communication between the

first devices and the second device (0032 and 0034).

As per claim 13, Ma teaches the step of creating at least one secret key

comprises: creating a plurality of secret keys distributed across the first devices by

creating a different secret key at each of the plurality of first devices [secure channel

(encrypted) are created between each device using identifying information from the first

devices, therefore each key will be different for each device for obvious security reason]

(0034);

and creating an identical plurality of secret keys at the second device [keys must match

in order for communication to occur between two devices] (0037).

As per claim 14, Ma teaches user interface [keypad] for generating a secret [PIN] by user input;

a memory [SIM] configured to store a generated secret for use in securing communications in a radio communications network comprising the apparatus and one or more additional apparatus (0032), wherein the stored secret is associated with an operational mode of the apparatus (0032; last sentence and 0037);

a radio transceiver [in smartphone] configured to communicate in the network; and a processor configured to access the secret stored in the memory and to create, using the accessed secret, a secret key for use in pairing the apparatus and the one or more additional apparatus to secure communication between them (0032-0033).

As per claim 15, Ma teaches the user interface [smart phone has keyboard for entering PIN which is stored in SIM] (0037) It is inherent that the PIN was at some time prior to the pairing entered by the user and stored in the SIM.

As per claim 17, Ma teaches wherein the stored secret is associated with a service provided by the device [secret must be known in order to gain service of the communication network] (0033).

As per claim 18, Ma teaches the radio transceiver is configured to receive a signal from any one of one or more additional apparatus (0034);

the processor is configured to determine that the signal is associated with an operational mode of the apparatus (0032); and

the processor is configured, in response to the determining, to access the secret in the memory in response to the received signal to create the secret key without user intervention (0032).

As per claim 19, Ma teaches the processor is operable to automatically create the secret key in response to the received signal [processor employs algorithms to the identifying data with keys to create a unique key] (0033).

As per claim 20, Ma teaches the stored secret [PIN] is independent of the origin of the received signal [the PIN is just made up by a user and stored in the SIM] (0032).

As per claim 21, Ma teaches the secret key is dependent upon the origin of the received signal [key is generated using identifying information of the first device, thus the key will depend on the device sending the signal] (0037).

As per claim 22, Ma teaches the received signal is a request (pairing request) and the secret key is dependent upon the content of the received request [key is generated using identifying information of the first device, thus the key will depend on the device sending the signal] (0037).

As per claim 23, Ma teaches the request includes a random value [number] used with at least the stored secret to create the secret key [first device passes random number to second device for authentication purposes which are an indication of usage] (0029).

As per claim 24, Ma teaches the processor is configured in a first mode to obtain a secret [PIN] by accessing the secret stored in the memory [SIM], is configured in a second mode to obtain a secret by enabling user input of data [receives PIN from user],

and is configured in the first mode and in the second mode to create, using the obtained secret, the secret key for use in pairing the apparatus and the one or more additional apparatus to secure communication between them (0037).

As per claim 26, Ma teaches the memory stores a device identifier [identifying information] for use with at least the stored secret to create the secret key (0037).

As per claim 27, Ma teaches a user input device [keypad] for programming the value of the stored secret [smart phone has keyboard for entering PIN which is stored in SIM] (0037) It is inherent that the PIN was at some time prior to the pairing entered by the user and stored in the SIM.

As per claim 28, Ma teaches the secret key is for use in securing all communications in the network [securely paired] (0032).

As per claim 29, Ma teaches the memory [SIM] is for storing a secret [PIN] for use in securing communications in the network between the device and a first additional device and between the device and a second additional device (0034), the processor is for accessing the secret in the memory and for creating, using the secret, a first secret key [key is created using identifying information of the first device] in common with the first additional device for securing communication between the device and the first additional device and a second secret key in common with the second additional device for securing communication between the device and the second additional device (0033). Ma teaches the process of securely pairing two devices can be extended to multiple devices, each carrying out their own secure pairing.

As per claim 30, Ma teaches a user interface for entering data [smart phone with keypad], wherein when the device participates in a different network controlled by a different device the user interface is usable to enter a secret stored at the different device and the processor is operable to create, using the entered secret, a secret key for securing communication (0032-0037). Ma teaches that the device holding the SIM card ultimately controls access to the wireless services. Ma teaches SIM are removable and can be transferred to other devices. Therefore when a control device gives up its SIM card, it can no longer function as the master device. This device then becomes the exemplary first device in the communication scheme. Ma teaches the first device gains access by secure pairing. It is therefore inherent that the smartphone without the SIM can perform the same authentication process that the PDA invokes as an example.

As per claim 34, Ma teaches an apparatus comprising:

a means for storing in a second apparatus which controls access to a radio communications network a secret generated at the second apparatus (0032) wherein the stored secret is associated with an operational mode of the apparatus (0032; last sentence and 0037);

means for making the stored secret available at a first apparatus without contemporaneous user input (0032); and

means for creating in the second apparatus, using the secret, a secret key for use in pairing the first apparatus and the second apparatus to secure communication between them (0032).

As per claim 35, Ma teaches a memory embodying a program for secure communication between a first and second apparatus comprising:

storing in a second apparatus [second device] which controls access to a radio communications network a secret generated at the second apparatus, wherein the stored secret [password] is associated with an operational mode of the second apparatus (0032);

making the stored secret available at a first apparatus without contemporaneous user input [told to (or known) by the user of the first apparatus which then inputs it into the first apparatus but does not need to be inputted into the second device; 0032; also taught in 0037 where it can be remembered and automatically input]; and

creating in the second apparatus, using the secret, a secret key for use in pairing the first and second apparatus to secure communication between them (0032).

As per claim 35, Ma teaches receiving a signal, at the second apparatus, from the first apparatus (0037);

determining that the signal is associated with the operational mode of the second apparatus [wants to access the carrier network for communication; a mode supported by the second device; 0037]; and

in response to the determining, automatically creating, without user intervention, the secret key [sends a key to the first device; 0037].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 16, 25, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ma in view of USP Application Publication 2004/0043790 to Ben-David et al, hereinafter Ben-David.

As per claims 3, 16, and 36 Ma does not explicitly teach the operational mode is a gaming mode. Ma teaches the use of PDA, smartphones, and the like to wirelessly communicate securely with others devices in short range. Ben-David teaches that PDA has numerous operating modes such as a gaming mode (0102). Ben-David teaches PDAs can operate gaming modes with Bluetooth and other wireless short range communication protocols. These PDAs seem to be in close function and nature to the system and method of Ma. For example two users within close proximity could play games together or separately. Ma also teaches the first device can use the second device to gain access to the carrier network for data communication. Games transmit data packets. Therefore it would have obvious to one of ordinary skill in the art at the

time of the invention to use the PDA's of Ben-David teaching in system of Ma because it adds to the level of user enjoyment. One of ordinary skill in the art knows the many features of PDAs and their ability to wirelessly communicate. Substituting various models would lead to predictable results.

As per claim 25, Ma does not explicitly teach the first mode is an interactive gaming mode and second mode is an idle mode. Ma teaches the use of PDA, smartphones, and the like to wirelessly communicate securely with others devices in short range. Ben-David teaches that PDA has numerous operating modes such as a gaming mode (0102) and sleep (idle) mode (0298). Ben-David, PDAs can operate gaming modes with Bluetooth and other wireless short range communication protocols. These PDAs seem to be in close function and nature to the system and method of Ma. They also offer a sleep mode to conserve battery life. Being able to communicate in both modes would greatly improve the convenience of the system. For example two users within close proximity could play games together or separately. And if one device is idling it could still be awaken to perform the needed duty of authentication. Therefore it would have obvious to one of ordinary skill in the art at the time of the invention to use the PDA's of Ben-David teaching in system of Ma because it adds to the level of user enjoyment and to the conversation of battery power. One of ordinary skill in the art knows the many features of PDAs and their ability to wirelessly communicate. Substituting various models would lead to predictable results.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431